HACKING WITH PYTHON3.0 BEGINNERS (I-II)

HINDI

DIGITAL DOWNLOAD हिंदी

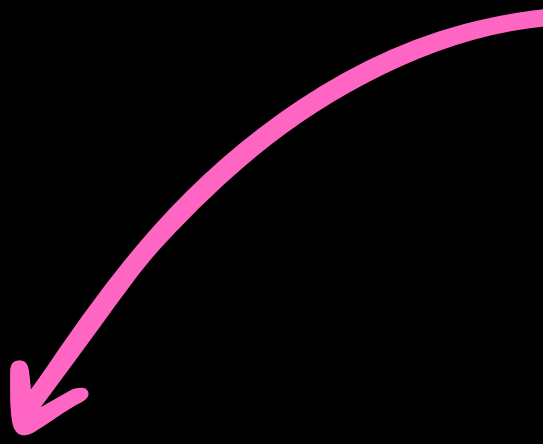
Hacking with Python - Beginner's Guide

Thanks for purchasing this Digital Download.

What's the success?

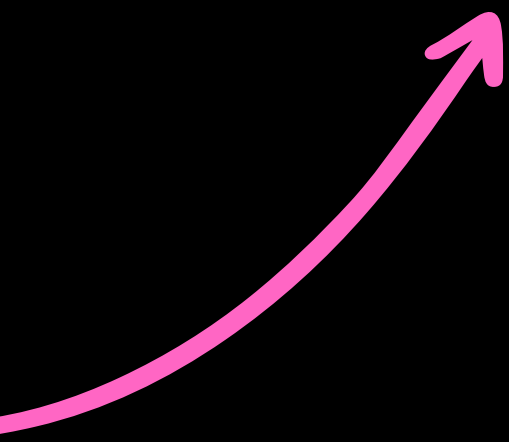
“We learn from failure, not from success!”
— Bram Stoker, Dracula

Please Keep this PDF in a safe place!



SUBSCRIBE TO FREE EBOOKS

www.cprogrammingbookinhindi.com



MACHHINDRA KALAN

Hacking with Python3.0 - Beginner's in HINDI

Copyright © 2017 by Machhindra Kalan

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Machhindra Kalan

Distributed to the book trade worldwide by Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

E-mail: machhi29@gmail.com, or

Visit: www.cprogrammingbookinhindi.com

For information on translations, please contact Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

Phone +91 86555-67778

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, the author shall not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this book.

This book
is dedicated
to those

who really wants
to be a

HACKING WITH PYTHON BEGINNERS (I-II) HINDI

INDEX OF CONTENTS

TABLE OF CONTENTS

PART - I

Introduction
Chapter 1: Basics of Hacking…….. 6
Chapter 2: How to Map Out Your Hacks……...13
Chapter 3: Cracking the Password……..25
Chapter 4: Spoofing Attacks to Fool Your Spoofing…….34
Chapter 5: Hacking into a Network Connection……...45
Chapter 6: Hiding and Finding Your IP Address……...55
Chapter 7: Keylogger 62
Chapter 8: Mobile Hacking…….68
Chapter 9: Hacking Tools That Make Your Hack Easier……74
Chapter 10: Tips to Keep Your Network Safe…….80

ADVANCED PART – 2

Introduction
Chapter 11: Basics of Hacking…….89
Chapter 12: Complete a Penetration Test ……94
Chapter 13: Physical Access to a System..... 98
Chapter 14: Hacking Passwords ……..……..... 103
Chapter 15: Social Engineering ……....108
Chapter 16: Wireless Network Attack ……113
Chapter 17: Man In The Middle Attack.....119
Chapter19: Tips for Beginners……...126

INTRODUCTION

हैकिंग एक ऐसा शब्द है जिसके कई अलग–अलग अर्थ होते हैं। ज्यादातर इसका इस्तेमाल नकारात्मक रोशनी में सुनने के लिए किया जाता है, जैसे कि जब एक ब्लैक हैट हैकर एक बड़ी कंपनी की वेबसाइट में घुस जाता है और बहुत सारी निजी जानकारी चुरा लेता है, या जब कोई आपके बैंक खाते में पैसे चोरी करता है। लेकिन हैकिंग के कई अन्य रूप भी हैं और आप अपने नेटवर्क को दूसरों से बचाने के लिए एक विधि के रूप में हैकिंग भी सीख सकते हैं जो जानकारी प्राप्त करना चाहते हैं।

इस पुस्तक Python के साथ हैकिंग की कुछ मूल बातें देखने के लिए समय बिताने जा रही है ताकि आप सिस्टम के माध्यम से नेविगेट कर सकें और अपने खुद के कुछ हैक कर सकें।

इस पुस्तक में, हम हैकिंग की कुछ बुनियादी बातों से शुरुआत करने जा रहे हैं, जैसे कि व्हाइट हैट और ब्लैक हैट हैकर के बीच का अंतर और कुछ ऐसी बातें जो आपको शुरू करने के लिए जानने की आवश्यकता होगी। इसके बाद हम कुछ अलग–अलग हैक को आगे बढ़ाएंगे, जिसमें आप पासवर्ड हैक, नेटवर्क हैक और Man in the middle (MID) को कुछ नाम शामिल कर सकते हैं।

इनमें से प्रत्येक आपको एक कंप्यूटर सिस्टम से अलग–अलग जानकारी प्राप्त करने की अनुमति देता है, और यदि आप इस बारे में अधिक जानना चाहते हैं कि आपका अपना निजी नेटवर्क कैसे काम करता है या इसे अन्य हैकर्स से कैसे बचा सकता है, तो इन हमलों में से कुछ करना सीखना एक बड़ा काम कर सकता है।

जब आप हैकिंग के साथ आने वाली कुछ बुनियादी बातों को सीखने के लिए तैयार हों और पायथन की मदद से ये हमले कैसे करें, तो इस किताब को देखें और जानें कि आपको इनमें से कुछ हैक करने की आवश्यकता

क्या है!

CHAPTER 1

BASICS OF HACKING

हैकिंग एक शब्द है जिसका अर्थ है कि प्रत्येक व्यक्ति जो इसे सुनता है, उसे अलग–अलग चीजें। किसी ऐसे व्यक्ति के लिए जो कोडिंग और कंप्यूटर की दुनिया में है, इसका मतलब कंप्यूटर के बारे में अधिक जानने और यह देखने का एक रोमांचक अवसर हो सकता है कि आप अपने कौशल के साथ कितनी दूर जा सकते हैं। किसी को जो निजी जानकारी प्राप्त करने के लिए देख रहा है और शायद इस प्रक्रिया में कुछ पैसे कमा सकता है,

हैकिंग सिस्टम पर आने और व्यक्तिगत जानकारी चुराने का एक तरीका है। और हम में से बाकी को, हैकिंग को आमतौर पर किसी को हमारे कंप्यूटर या हमारे सिस्टम पर प्राप्त करने और जानकारी लेने के रूप में देखा जाता है कि उन्हें प्राप्त करने की अनुमति नहीं है।

हालांकि, ये तरीके हो सकते हैं कि हैकिंग का उपयोग किया जाता है, हैकिंग की प्रक्रिया को आमतौर पर सॉफ़्टवेयर के टुकड़े या कंप्यूटर का उपयोग करने के कार्य के रूप में संदर्भित किया जाता है, जो इसका उद्देश्य नहीं था। कभी–कभी यह आपके अपने डिवाइस की सुरक्षा के लिए किया जाता है, यह जानने के लिए कि डिवाइस कैसे काम करता है, डिवाइस को सुधारें, या एक ऐसी प्रणाली को प्राप्त करने के लिए जिसे आप चालू नहीं कर सकते।

तीन मुख्य प्रकार के हैकर्स हैं जो आपको मिलेंगे और जबकि वे सभी एक ही तरीके का उपयोग करने जा रहे हैं जो वे एक सिस्टम से चाहते हैं, वे सभी ऐसा करने के लिए अलग–अलग कारण हैं। हैकिंग के लिए तीन मुख्य श्रेणियों में शामिल हैं:

1. ब्लैक हैट: यह हैकिंग का प्रकार है जो ज्यादातर लोग पहले सोचते हैं। ये बुरे लोग हैं, आपराधिक हैकर जो किसी दुर्भावनापूर्ण उद्देश्य के लिए एक सिस्टम पर मिलेंगे। वे कर सकते हैं

बस बैंकिंग और अन्य व्यक्तिगत जानकारी चुराने के लिए एक निजी प्रणाली में प्रवेश करें या वे एक बड़े व्यवसाय की प्रणाली पर प्राप्त कर सकते हैं और फिर बहुत अधिक अराजकता का कारण बन सकते हैं। आमतौर पर, इस प्रकार के हैकर्स फ़ाइलों को हटाने, उपकरणों को संशोधित करने या हैक को पूरा करने के लिए डेटा चोरी करने जा रहे हैं।

2. सफेद हैट: इन्हें आमतौर पर हैकिंग में अच्छे लोगों के रूप में देखा जाता है। ये वे हैं जो अपने स्वयं के सिस्टम, या किसी के सिस्टम को हैक करने से बचाने के लिए काम कर रहे हैं। कई बड़े संगठन और यहां तक कि अस्पताल जैसे स्थान व्यक्तिगत और वित्तीय जानकारी की सुरक्षा में मदद करने के लिए सफेद टोपी हैकर्स को काम पर रखेंगे। उनका काम एक सिस्टम पर होना है और उन तरीकों को खोजने की कोशिश करना है जो सिस्टम पर पाने के लिए ब्लैक हैट हैकर्स कोशिश कर सकते हैं, और फिर इन मुद्दों को ठीक करने के लिए सिस्टम पर किसी को भी होने से रोकना चाहिए जो वहां नहीं होना चाहिए।

3. ग्रे हैट: यह एक हैकर है जो ऊपर सूचीबद्ध दोनों के बीच में कहीं है। ये व्यक्ति शोषण करने या करने के लिए अवैध और कानूनी दोनों तरह की तकनीकों का इस्तेमाल करने वाले हैं एक प्रणाली में सुधार। आमतौर पर, ग्रे हैट हैकर किसी व्यवसाय या किसी अन्य व्यक्ति की प्रणाली पर कोशिश करने और प्राप्त करने जा रहा है, लेकिन उनके पास दुर्भावनापूर्ण इरादे नहीं हैं और वे सिस्टम के मालिक को बताएंगे कि वे क्या खोजने में सक्षम थे। अक्सर ये हैकर्स सिर्फ यह देखने के लिए उत्सुक होते हैं कि क्या वे एक ऐसी प्रणाली पर पहुँच सकते हैं जिसकी उनके पास पहुँच नहीं है, लेकिन वे वास्तव में जानकारी का उपयोग नहीं करना चाहते हैं।

इस गाइडबुक में, हम हैकिंग के बारे में बात करने के लिए कुछ समय बिताने जा रहे हैं और कुछ ऐसी तकनीकें जो आप सीख सकते हैं

जब आपके सिस्टम की सुरक्षा की बात आती है। उस के साथ, अवैध हैकिंग या किसी सिस्टम पर प्राप्त करने का कोई भी प्रयास जिसे आपके पास होने की अनुमति नहीं है, इस गाइडबुक में सम्मिलित या प्रोत्साहित नहीं किया गया है। इन तकनीकों और युक्तियों का उपयोग करना आपके स्वयं के व्यक्तिगत कंप्यूटर या नेटवर्क की सुरक्षा के लिए बहुत अच्छा है, लेकिन बिना अनुमति के अन्य प्रणालियों तक पहुंचने के लिए उनका उपयोग करना अवैध है और कानून द्वारा दंडनीय हो सकता है। क्या कौशल मुझे चाहिए

हैकिंग शुरू करें?

हैकिंग एक कौशल है जिसे मास्टर करने के लिए कुछ अभ्यास की आवश्यकता होगी, लेकिन इसे सीखना बहुत मुश्किल नहीं है। जब तक आप परिचित हैं कि आपका कंप्यूटर कैसे काम करता है और आप कुछ निर्देशों का पालन कर सकते हैं, जिन्हें हम इस पुस्तक में रेखांकित करेंगे, तो आप आसानी से इनमें से कुछ हैक्स का उपयोग अपने सिस्टम पर कर पाएंगे। इस पुस्तक में कोड्स को करने के लिए आपके पास एक चीज़ जो होनी चाहिए, वह है पायथन के साथ कोड करने की एक बुनियादी समझ। अगर आपको पता नहीं है कि कोड कैसे बनाया जाता है

पायथन के साथ अभी तक, मैं पायथन प्रोग्रामिंग को पढ़ने का सुझाव देता हूं: ए स्टेप बाय स्टेप बिगिनर: एस गाइड टू कोडिंग विथ पायथन विथ 7 डेज या इससे कम! ताकि आप समझ सकें कि हम अलग–अलग हैक के बारे में क्या बात करते हैं।

कंप्यूटर के कुछ अन्य कौशल जिन्हें आपको पायथन के साथ हैक करना शुरू करना होगा:

- कंप्यूटर कौशल: हैकिंग में एक विशेषज्ञ की जरूरत नहीं है आपको मूल बातें से थोड़ा अधिक करने में सक्षम होने की जरूरत है। आपको यह जानना होगा कि रजिस्ट्री की कुछ चीजों को कैसे संपादित किया जाए फ़ाइलें, कैसे एक नेटवर्क के साथ काम करने के लिए, और हैकिंग का काम करने के लिए विंडोज में कैसेन लाइनों के साथ काम करना है।

- नेटवर्किंग कौशल: अधिकांश हमले जो आप करना चाहते हैं, वे होंगे ऑनलाइन इसलिए नेटवर्किंग की कुछ समझ होना जरूरी है अवधारणाओं और शर्तों। यदि आप वीपीएन, डीएनएस, पोर्ट्स,

राउटर और अन्य नेटवर्किंग शर्तों के बारे में नहीं जानते हैं, तो आप उन्हें शुरू करने में मदद करने के लिए उन्हें सीखने में कुछ समय बिताना चाहते हैं।

- लिनक्स ओएस: लिनक्स ऑपरेटिंग सिस्टम मैक और विंडोज ऑपरेटिंग सिस्टम की तुलना में हैकिंग की बात आती है तो इसका उपयोग करना सबसे आसान है। उपलब्ध सबसे अच्छे हैकिंग टूल में से कई लिनक्स का उपयोग करेंगे और इस ऑपरेटिंग सिस्टम में पहले से ही इसके अंदर पायथन होगा।

- वर्चुअलाइजेशन: इससे पहले कि आप किसी सिस्टम या नेटवर्क पर हमला करना शुरू करें, आपको यह सुनिश्चित करने की आवश्यकता है कि आप क्या कर रहे हैं, या ऐसी बहुत सारी गलतियाँ होंगी जो सिस्टम एडमिनिस्ट्रेटर के खिलाफ होगी और आप पकड़े जाएंगे। आपको करना पड़ सकता है समय से पहले हैक को बाहर निकालने में मदद करने के लिए VMWare वर्कस्टेशन जैसे कुछ सॉफ़्टवेयर का उपयोग करें।
- **Wireshark:** यह जानने के लिए कि मदद करने के लिए Wireshark का उपयोग करना एक अच्छा विचार है। यह सबसे अच्छा स्निफर्स में से एक है और साथ ही एक प्रोटोकॉल विश्लेषक भी आपकी मदद करने के लिए है।
- स्क्रीप्टिंग स्किल्स: अगर आपको अपनी सक्रिप्ट बनाने और यहां तक कि उन्हें एडिट करने का कुछ अनुभव है, तो आप हैकिंग के लिए खुद के टूल्स बना पाएंगे और इसे बना सकते हैं, इसलिए आपको टूल्स या अन्य पर भरोसा करने की जरूरत नहीं है सॉफ्टवेयर आपकी मदद करने के लिए। यह आपकी हैकिंग को अधिक विश्वसनीय और सफल बना सकता है।
- डेटाबेस कौशल: डेटाबेस तक पहुंचने और इसके माध्यम से प्राप्त

करने के लिए, आपको यह समझने की आवश्यकता है कि ये कार्य कैसे करते हैं इसका मतलब है कि Oracle और MySQL जैसे विकल्पों में कुछ अनुभव होने से आपको मदद मिल सकती है।

- रिवर्स इंजीनियरिंग: यह जानने के लिए एक अच्छी बात है कि इसका उपयोग कैसे करें क्योंकि यह आपको मैलवेयर को एक उपकरण में बदलने की अनुमति देता है जिसे आप हैकिंग के लिए उपयोग कर सकते हैं।

यह बहुत सी जानकारी की तरह लग सकता है जिसे आपको हैकिंग का काम करने के लिए सीखना और समझना होगा, लेकिन यह सब महत्वपूर्ण है। हैकिंग एक जटिल उपाय है क्योंकि आप अपने सिस्टम को एक ऐसे तरीके से force करने की कोशिश कर रहे हैं जिसे आप नेटवर्क में किसी और के बिना नहीं जानते हैं कि आप वहां हैं। इसके लिए बहुत काम करने की आवश्यकता हो सकती है, लेकिन यह तब काम आएगा जब आप अपना पहला हैक शुरू करने के लिए तैयार होंगे।

CHAPTER 2

MAP OUT YOUR HACKS

एक बार जब आपके पास कुछ ज्ञान होता है, जिसे आपको हैक के साथ शुरू करने की आवश्यकता होती है, तो यह आपके हमले की योजना बनाने का समय है।

हर हैकर को हमले की योजना बनाने की जरूरत होती है, इस बात का अंदाजा है कि जब वे हैक शुरू करते हैं तो वे क्या करना चाहते हैं और यहां तक कि वे कमजोरियों का पता लगाने में सक्षम होने जा रहे हैं। यदि आप नेटवर्क के अंदर बहुत अधिक गड़बड़ करते हैं, तो कोई है

यह पता लगाने के लिए कि आपके त्वरित और प्रभावी होने का सबसे अच्छा तरीका है, आपके हैक को काम करने के लिए और आपकी हैकिंग को मैप करने के लिए ऐसा करने जा रहा है।

जब आपके नेटवर्क के माध्यम से जा रहे हैं और यह पता लगाने की कोशिश कर रहे हैं कि कुछ भेद्यताएं कहां हैं, तो आपको सिस्टम पर प्रत्येक प्रोटोकॉल को एक बार में जांचने की आवश्यकता नहीं है। यह सिर्फ भ्रमित करने वाली चीजें हैं और आप पा सकते हैं कि कुछ गलत है, लेकिन आपको नहीं पता होगा कि यह क्या है क्योंकि बहुत अधिक चल रहा है। जाने का सबसे अच्छा तरीका

भेद्यताओं (Vulnerability) की जाँच करने के बारे में है कि प्रत्येक भाग को स्वयं के माध्यम से जाना और परीक्षण करना है ताकि आप देख सकें कि कोई भी समस्या कहाँ से आती है।

अपने हैक को मैप करते समय, आपको केवल एक एप्लिकेशन या एक सिस्टम के साथ शुरू करना चाहिए जिसे सबसे अधिक सहायता की आवश्यकता है। तब आप सूची के माध्यम से जा सकते हैं और उन सभी पर जांच कर सकते हैं जब तक कि आप सब कुछ पूरा नहीं कर लेते। यदि आप अनिश्चित हैं कि आप किस सिस्टम के साथ काम करना चाहते

हैं, तो आप इन सवालों को पूछ सकते हैं:

- अगर किसीने ने सिस्टम पर एक हमला करने की कोशिश की, जो हिस्सा खत्म हो जाएगा जिससे सबसे ज्यादा परेशानी होगी या जो हिस्सा खत्म हो जाएगा अगर आप उस पर जानकारी खो देते हैं तो वास्तव में कितना मुश्किल होगा?
- अगर आप पर सिस्टम अटैक होता है, तो सिस्टम का कौन सा हिस्सा सबसे कमजोर है? (इसलिए, वह है जो आपके हैकर को उपयोग करने की सबसे अधिक संभावना है)
- क्या सिस्टम का कोई हिस्सा ऐसा है जो उस अच्छी तरह से प्रलेखित नहीं है या जो मुश्किल से जांचा जाता है? क्या वहां भी कुछ ऐसे हैं जो आपसे परिचित नहीं हैं (या आपने भी नहीं अतीत में देखा)?

एक बार जब आप इनमें से कुछ सवालों के जवाब दे सकते हैं, तो आप उन कुछ प्रणालियों और अनुप्रयोगों की अच्छी सूची बना पाएंगे, जिन्हें आप पहले से शुरू करना चाहते हैं। इस प्रक्रिया के दौरान कुछ अच्छे नोट्स रखें ताकि चीजों को रखना आसान हो जाए क्योंकि आप अलग–अलग प्रणालियों से चलते हैं और आपको चीजों को दस्तावेज करने की आवश्यकता होगी यदि आप मुद्दों पर चलते हैं ताकि आप उन्हें बाद में ठीक कर सकें।

Getting Your Project

अब जब आपके पास कुछ ऐसी प्रणालियाँ और अनुप्रयोग शुरू हो गए हैं जिन्हें आप चलाना चाहते हैं, तो आपको यह सुनिश्चित करने की ज़रूरत है कि आपके पास सब कुछ है।

आप इन परीक्षणों को हर उस चीज़ पर चलाना चाहते हैं जो आपके कंप्यूटर के अंदर है, यह सुनिश्चित करने के लिए कि यह सुरक्षित है। शामिल करने के लिए आपको जिन चीजों को याद रखना चाहिए उनमें से कुछ हैं:

- आपके राउटर और आपके स्विच
- कुछ भी जो सिस्टम से जुड़ा है इसमें टैबलेट, वर्कस्टेशन जैसी चीजें शामिल होंगी लैपटॉप।
- सर्वर और क्लाइंट वाले सहित सभी ऑपरेटिंग सिस्टम।
- वेब सर्वर, एप्लिकेशन और डेटाबेस।
- सुनिश्चित करें कि फ़ायरवॉल सभी जगह हैं।
- ईमेल, फ़ाइल और प्रिंट सर्वर। आप इस प्रक्रिया के दौरान कई अलग–अलग परीक्षण चलाने जा रहे हैं, लेकिन यह हो रहा हैं।

यह सुनिश्चित करने के लिए कि आप जाँच करते हैं।
सिस्टम पर सब कुछ और उन कमजोरियों को ढूंढें जो वहां हैं। अधिक डिवाइस और सिस्टम जिनकी आपको आवश्यकता है

जाँच करें, परियोजना को व्यवस्थित करने में अधिक समय लगेगा। आप सूची में कुछ बदलाव कर सकते हैं और उन विकल्पों को चुन सकते हैं जो आपको लगता है कि कुछ समय बचाने और अपने सिस्टम को सुरक्षित रखने के लिए सबसे महत्वपूर्ण हैं।

हैक करने का सबसे अच्छा समय कब है?

एक बड़ा सवाल जो बहुत से लोग पूछेंगे कि हैक करने का सबसे अच्छा समय कब है। जब आप अपने ऊपर काम कर रहे होते हैं

लक्ष्य, आपको आश्चर्य हो सकता है कि जब आप सिस्टम पर हो सकते हैं, तो अन्य लोगों को परेशान किए बिना सबसे अधिक जानकारी प्राप्त करने के लिए हैक करना चाहिए। यदि आप अपने निजी कंप्यूटर पर काम कर रहे हैं, तो आप इन हमलों को किसी भी समय कर सकते हैं जो आपके लिए काम करता है। लेकिन अगर आप एक बड़े सिस्टम पर काम कर रहे हैं जहां अन्य लोग जानकारी का उपयोग करेंगे, जैसे कि व्यवसाय का नेटवर्क, आपको उस समय के बारे में सावधान रहना चाहिए जो आप हैक के लिए चुनते हैं।

यदि अन्य डिवाइस नेटवर्क पर हैं या आप व्यवसाय नेटवर्क का उपयोग कर रहे हैं, तो आप समय लेने की जरूरत है जहां आप कंपनी के नियमित व्यावसायिक कार्यों में बड़ी गड़बड़ी नहीं करेंगे। उदाहरण के लिए, यदि व्यवसाय लंच ऑवर के दौरान सबसे व्यस्त रहता है, तो इस समय से ठीक पहले इनमें से एक हमला करना अच्छा नहीं होगा क्योंकि यह संभव है कि आप उस सेवा में हस्तक्षेप करेंगे जो ग्राहकों को मिलती है। बल्कि, ऐसे समय के साथ जाएं जो धीमा है, जैसे कि रात में, ताकि आपको काम करने की बहुत अधिक स्वतंत्रता हो किसी और को बाधित किए बिना हैक।

मेरे सिस्टम के अलावा अन्य क्या देख सकते हैं?
अब जब हम एक हैक करने के लिए तैयार हैं, तो आपको जांचने और देखने की जरूरत है कि दूसरे आपके नेटवर्क के बारे में क्या देख सकते हैं। एक अच्छा हैकर आपके सिस्टम पर समय से पहले कुछ शोध करने जा रहा है और वे कमजोरियों को उजागर करने वाली कई व्यक्तिगत जानकारी का पता लगाने के लिए चारों ओर खोज करेंगे। यदि आप सिस्टम के मालिक हैं, तो आप इनमें से कुछ स्पष्ट हिस्सों को याद कर सकते हैं, इसलिए आपको इसे एक नए ब्रांड से देखना होगा,

यह देखिए कि एक हैकर क्या देखता है, बजाय इसके कि आप क्या सोचते हैं।

कुछ विकल्प हैं जो आप इन ट्रेल्स को इकट्ठा करते समय उपयोग करने में सक्षम होंगे, लेकिन एक ऑनलाइन खोज पहले स्थानों में से एक है जिसे आपको जांचना चाहिए। किसी भी जानकारी को जानने के लिए आपको बस ऑनलाइन एक खोज करने की आवश्यकता होगी
वहाँ है कि आप से संबंधित है। फिर आप यह जांचने के लिए काम कर सकते हैं कि कोई व्यक्ति आपके या आपके सिस्टम के बारे में क्या देख पाएगा। इन मुद्दों में से कुछ को खोजने में मदद करने के लिए एक स्थानीय पोर्ट स्कैनर।

यह केवल एक मूल प्रकार की खोज है

आप कर सकते हैं, लेकिन आपको थोड़ा और गहरा करने की आवश्यकता है, या आप कुछ ऐसी चीजों को याद करेंगे जिन्हें आपका कंप्यूटर दुनिया में भेज सकता है। कुछ अन्य चीजें जो आपको शामिल करनी चाहिए:

- कोई भी संपर्क जानकारी जो किसी और को यह देखने देगी कि

कौन व्यवसाय के साथ काम कर रहा है। बाहर की जाँच करने के लिए कुछ अच्छे स्थानों में USSearch, ZabaSearch, और ChoicePoint शामिल हैं।

- किसी भी प्रेस विज्ञप्ति के माध्यम से देखें जिसमें बड़े बदलावों की बात की गई है।
- कोई भी अधिग्रहण या विलय जो कंपनी के लिए चारों ओर आया है।
- SEC दस्तावेज़ जो उपलब्ध हैं।
- पेटेंट या ट्रेडमार्क में से कोई भी कंपनी के स्वामित्व में है।
- निगमन फाइलिंग जो अक्सर एसईसी के साथ होती है, लेकिन कुछ मामलों में, वे अन्य स्थानों में भी हो सकती हैं।

यह देखने के लिए बहुत सारी जानकारी है, लेकिन यह एक हैकर के लिए मूल्यवान हो सकता है और आपको यह निर्धारित करने में सक्षम होने की आवश्यकता है कि कैसे वहाँ के लिए बहुत उपलब्ध है हैकर उपयोग करने के लिए। एक कीवर्ड खोज इसे काट नहीं करेगी; आपको इस जानकारी को खोजने के लिए और भी गहरे जाने और कुछ उन्नत खोज करने की आवश्यकता है। इस जानकारी में से कुछ को लिखने के लिए समय निकालें ताकि आपको इस बात का बेहतर अंदाजा हो कि नेटवर्क कितना बड़ा है, कौन सी जानकारी को जनता तक पहुंचाया जा रहा है, और अन्य कमजोरियां जो आपके नेटवर्क को नुकसान पहुंचा सकती हैं।

नेटवर्क को मैप करना

एक बार आपके पास यह सब जानकारी होने के बाद, यह आपके नैतिक हैक पर काम करने का समय है। एक नेटवर्क जिसमें बहुत सारी जानकारी है और उस पर डिवाइस की रक्षा करना सबसे मुश्किल होगा क्योंकि आपके पास बहुत सारे लोग हैं जो इसका उपयोग कर रहे हैं समय

इसलिए आपको यह सुनिश्चित करने की आवश्यकता है कि सभी डिवाइस सुरक्षित हैं और लोग अनुचित तरीके से इनका उपयोग नहीं कर रहे हैं।

तो, यह नेटवर्क के माध्यम से जाने और मैप करने का समय है। इससे पदचिह्न को देखना संभव हो जाता है कि आपका सिस्टम या नेटवर्क दूसरों को देखने के लिए ऑनलाइन छोड़ रहा है। Whois शुरू करने के लिए एक शानदार जगह है। यह मूल रूप से यह देखने के लिए डिज़ाइन किया गया था कि क्या डोमेन नाम आपके उपयोग के लिए उपलब्ध है

या नहीं, लेकिन अगर आप एक डोमेन नाम के पंजीकरण के बारे में जानकारी देखना चाहते हैं तो यह एक अच्छी जगह है। यदि आप यहां पर खोज करते हैं और नोटिस करते हैं कि आपका डोमेन नाम दिखाता है, तो यह आपके परिवर्तनों को बढ़ाता है जो कंपनी के बारे में संपर्क जानकारी, जैसे कि ईमेल पते और कंपनी चलाने वालों के नाम इस साइट पर प्रसारित किए जा रहे हैं।
Whois एक विशेष डोमेन पर पाए जाने वाले सभी DNS सर्वरों के बारे में और साथ ही आपके तकनीकी समर्थन के बारे में थोड़ी जानकारी दे सकता है।

सेवा प्रदाता उपयोग करता है। एक जगह जिसे आपको वास्तव में देखने की आवश्यकता है वह DNSstuf में है ताकि आप बहुत सारी जानकारी का पता लगा सकें, जिसमें आपके डोमेन के बारे में दिखाया गया है:

- होस्ट कैसा है इसकी जानकारी इस विशेष नाम के लिए सभी ईमेल को संभालने में सक्षम है।
- जहाँ सभी Hosts स्थित हैं।
- कुछ सामान्य जानकारी जो डोमेन के पंजीकरण के बारे में हैकर के लिए उपयोगी हो सकती है।

- इसके साथ स्पैम होस्ट है या नहीं इसकी जानकारी।

यह उन साइटों में से एक है जो आप इस जानकारी को जानने के लिए देख सकते हैं और इनमें से कुछ को देखना एक अच्छा विचार है। यह उन सूचनाओं पर एक अच्छी शुरुआत देने में मदद करता है जो आपके डोमेन और आपकी कंपनी के लिए ऑनलाइन हो सकती हैं, लेकिन कुछ अन्य स्थान भी हैं जिनकी आपको जाँच करनी चाहिए:

Google फ़ोरम और समूह

ये आपके नेटवर्क के बारे में अधिक जानकारी प्राप्त करने के लिए हैकर्स के लिए बहुत अच्छी जगह हैं, और आप इस बात से आश्चर्यचकित हो सकते हैं कि मंचों में यह जानकारी कितनी पोस्ट की गई है, भले ही आप कभी नहीं
इसे पोस्ट करने वाले थे। आपके द्वारा पोस्ट की गई जानकारी के आधार पर, आपकी सुरक्षा के साथ काम करने के लिए आपके पास बहुत सारे मुद्दे हो सकते हैं। इस साइट पर डोमेन नाम, आईपी पते और उपयोगकर्ता नाम जैसी चीजों को ढूंढना संभव है और यह जानकारी प्राप्त करने के लिए आपको बस अपनी कंपनी या डोमेन नाम की सरल खोज करनी होगी।
अच्छी खबर यह है कि यदि आप इस जानकारी को खोजते हैं, तो आप इसे और अधिक लोगों को खोजने से पहले हटा पाएंगे और अपनी सुरक्षा के माध्यम से प्राप्त करने का प्रयास करेंगे। आपको यह सुनिश्चित करना चाहिए कि आपके पास कुछ है ऐसा करने के लिए सही क्रेडेंशियल्स के स्थान पर (लेकिन यदि आप नेटवर्क के मालिक हैं या आप कंपनी के आईटी विभाग में काम करते हैं, तो आपके पास ये होंगे)। फिर आप इन साइटों पर सहायता कर्मियों के लिए क्षेत्र में जा सकते हैं और फिर उन्हें साइट से हटाने के लिए एक रिपोर्ट दर्ज कर सकते हैं।

Doing the System Scan

जैसा कि आप ऊपर दिए गए चरणों के माध्यम से जाते हैं, लक्ष्य यह पता लगाना है कि आपका नेटवर्क पहले से ही कितना ऑनलाइन है ताकि आप कर सकें।

देखें कि हैकर्स अपने स्वयं के हमलों में से एक को शुरू करने के लिए कहां देख सकते हैं। यह कुछ समय लेने वाला है क्योंकि हैकर सिस्टम पर प्राप्त करने के लिए बहुत अधिक दृढ़ होने जा रहा है, इसलिए आपको उन्हें करने से पहले तेज और सक्षम होने की आवश्यकता है। अब जब आपके पास यह जानकारी है, तो यह सुनिश्चित करने के लिए कुछ और चीजें करने का समय है कि आपके सिस्टम का ठीक से ध्यान रखा जाए। ये स्कैन कुछ कमजोरियों को दिखाने जा रहे हैं जो सिस्टम में हैं इसलिए आपको पता है कि आपके नेटवर्क की सुरक्षा कहाँ से शुरू करें। कुछ स्कैन जो आप अपने नेटवर्क की सुरक्षा के लिए कर सकते हैं:

1. हम किसके बारे में ऊपर की तरह बात करते हैं और फिर होस्टनाम और आईपी पते देखें। देखें कि उन्हें इस साइट पर कैसे रखा गया है और आप उस समय की जानकारी को सत्यापित करने के लिए भी समय निकाल सकते हैं।
2. अब आपके कुछ आंतरिक होस्ट को स्कैन करने का समय है, ताकि आप देख सकें कि उपयोगकर्ता सिस्टम पर क्या एक्सेस कर पा रहे हैं। यह संभव है कि हैकर नेटवर्क के भीतर से आ सकता है या वे किसी से प्राप्त करने के लिए कुछ क्रेडेंशियल्स प्राप्त कर सकते हैं कर्मचारी जो सावधान नहीं है, इसलिए सुनिश्चित करें कि सभी के पास कंपनी में जहां वे हैं, उसके आधार पर सही क्रेडेंशियल्स हैं।
3. अगली चीज जो आपको करने की आवश्यकता होगी वह है सिस्टम की पिंग उपयोगिता की जांच करना। कभी–कभी एक

तृतीय–पक्ष उपयोगिता इसके साथ मदद करेगी ताकि आप एक समय में पिंग करने के लिए एक से अधिक पते प्राप्त कर सकते हैं। SuperScan उपयोग करने के लिए एक बढ़िया विकल्प है। यदि आप अपने गेटवे आईपी पते के नाम के बारे में अनिश्चित हैं, तो आप www.whatismyip.com साइट पर भी जा सकते हैं।

4. और अंत में, आपको उन सभी पोर्ट की मदद से अपने सिस्टम का एक बाहरी स्कैन करना होगा जो खुले हैं।
   आप सुपरस्कैन को फिर से खोल सकते हैं और फिर देख सकते हैं कि कोई क्या है हो सकता है कि Wireshark की मदद से नेटवर्क पर देखा जा सके।

ये स्कैन आपको यह पता लगाने में मदद करने के लिए सभी शानदार हैं कि आपका आईपी पता ऑनलाइन क्या भेज रहा है और जब वे आपके सिस्टम पर आने की कोशिश करते हैं तो हैकर्स क्या देख रहे होंगे। एक हैकर मूल रूप से कुछ ऐसे ही कदम उठा सकता है, जो आपने सिस्टम में किए थे और यह देखने के लिए कि क्या चल रहा है

आगे–पीछे होने वाले ईमेलों को देखने के लिए, और दूरस्थ पहुँच के लिए सही जानकारी प्राप्त करने का तरीका भी सीखें। इन स्कैन का बिंदु यह पता लगाना है कि हैकर कहां से मिल सकता है ताकि आप उन्हें बंद कर सकें और सिस्टम को सुरक्षित रख सकें।

एक बार जब आपको यह पता चल जाए कि हैकर आपके नेटवर्क पर कैसे पहुंच सकता है, तो सटीक तरीके से यह सीखना आसान है कि हैकर आपके निशाने पर आना चाहेगा। वे सबसे आसान तरीका चुनने की संभावना रखते हैं जो वे दूसरों से छिपे हुए रहते हैं सिस्टम पर। यह पहली

चीज होनी चाहिए कि आप यह सुनिश्चित करने के लिए कुछ अतिरिक्त सुरक्षा जोड़ने की कोशिश करें कि एक हैकर इस जानकारी से बाहर रहता है।

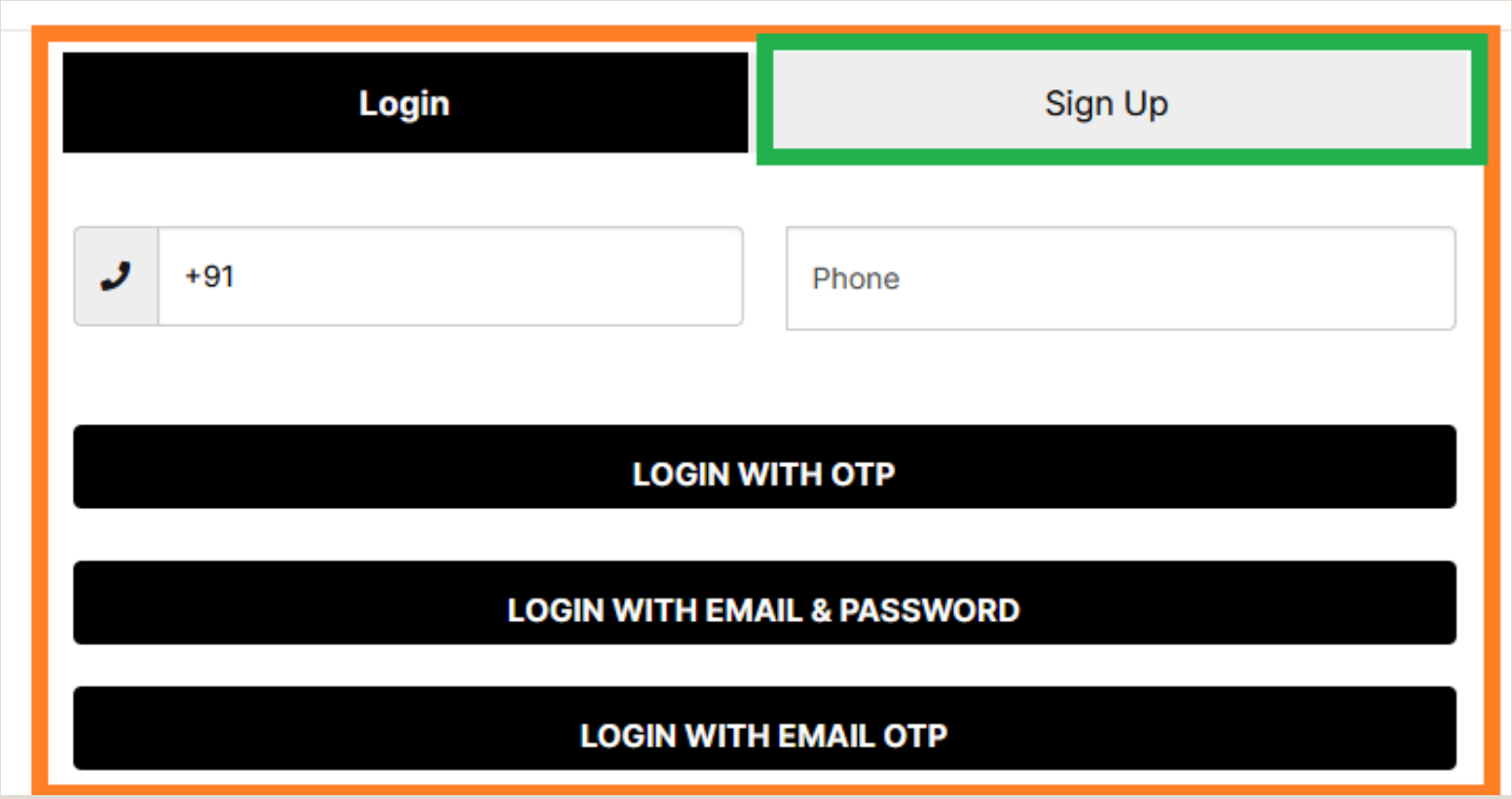
ये स्कैन कुछ ऐसे हैं जिन्हें आपको नियमित रूप से करते रहना होगा। सिर्फ एक बार काम करना काफी नहीं है। जैसा कि आप नेटवर्क का अधिक उपयोग करते हैं या समय के साथ अधिक लोगों को इसमें जोड़ते हैं, जो जानकारी बाहर भेजी जाती है वह बदल सकती है और हैकर्स की तलाश हमेशा रहती है। नियमित रूप से इस तरह के स्कैन करने से आप अपने सिस्टम की सुरक्षा कर सकते हैं और हैकर्स जो संबंधित नहीं है इसे बाहर रख सकते हैं।

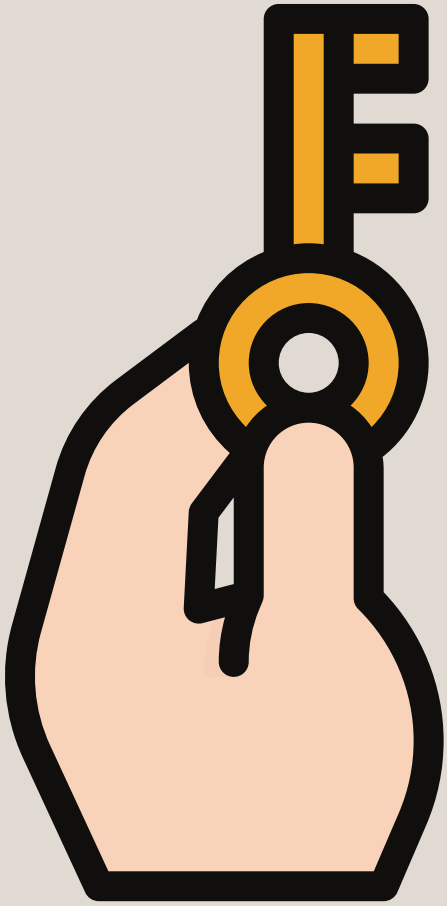
HOW TO GET COMPLETE PDF EBOOK

Pay Paytm

कोई भी **2 Ebooks** खरीदने पर **20%** डिस्काउंट- **India20**

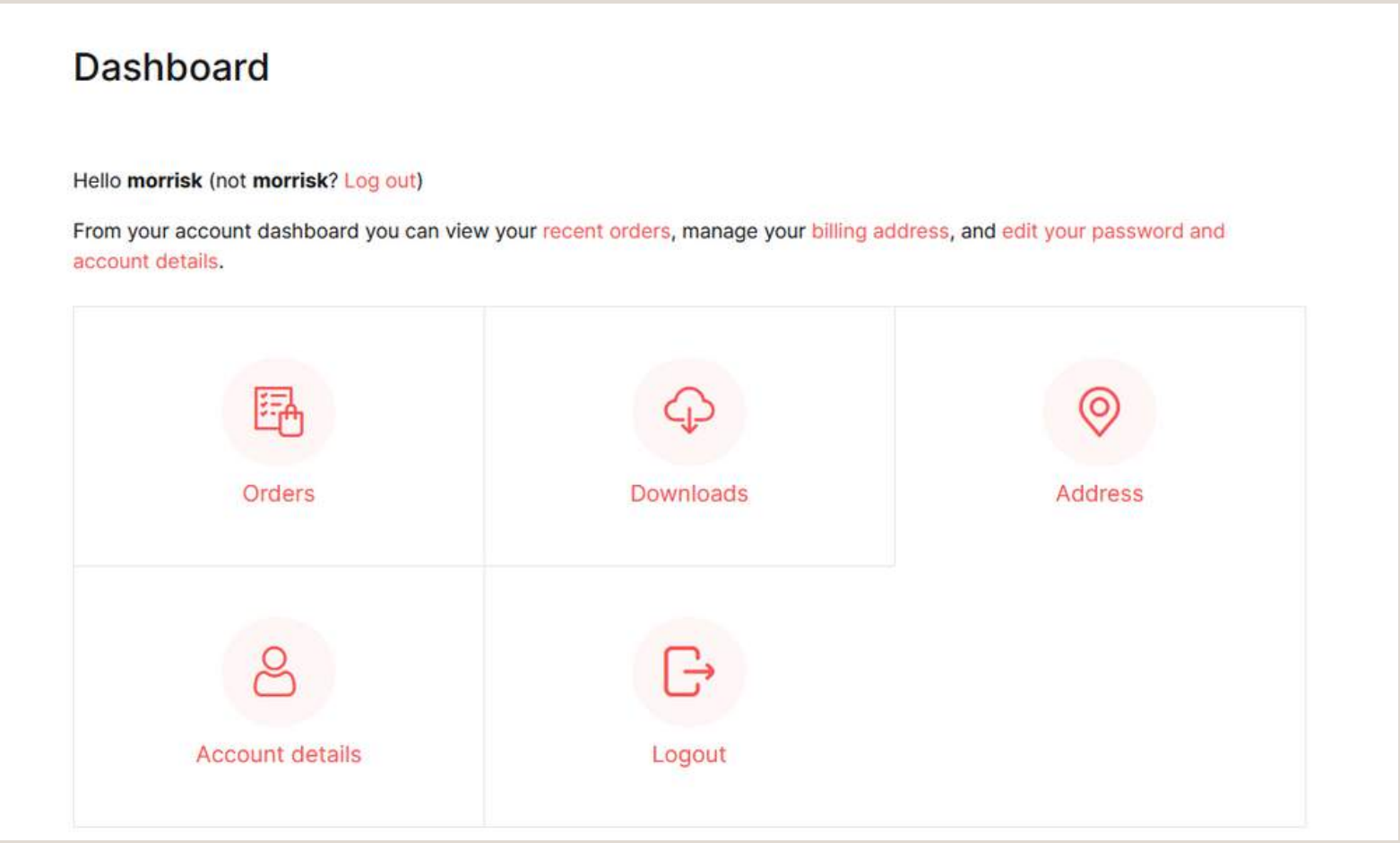
Buy Now पर क्लिक करने पर आपको **चेकआउट पेज** पर लॉगिन फॉर्म पर पहिले ईमेल से लॉगिन करना होगा।





Login Succesfull के बाद आपको पेमेंट करके Ebooks वही से डाउनलोड कर सकते है।

उसके बाद आप **My Account** पेज पर जाकर **Download** में Ebooks डाउनलोड कर सकते है।



Thank you